WHAT IS CLAIMED IS:

1. An apparatus, comprising:

a cartridge having an information storage media therein, and having a unique identifier associated therewith;

a receiving section into which said cartridge can be removably inserted; and

a further section operatively coupled to said receiving section;

said receiving section being responsive to an occurrence of a predetermined event when said cartridge is removably inserted therein for transmitting to said further section public key information and an encrypted segment, where said encrypted segment has been formed through asymmetric encryption with a private key of a data segment which includes said unique identifier; and

said further section decrypting said encrypted segment as a function of said public key information, in order to obtain access to said unique identifier.

2. An apparatus according to Claim 1,

wherein said further section includes a public key list containing a plurality of public keys;

wherein said public key information identifies one of said public keys in said list; and

wherein said further section uses said one public key to effect said decryption of said encrypted segment.

3. An apparatus according to Claim 1,

wherein said private key, said public key information and said unique identifier are stored in said cartridge during manufacture thereof; and

wherein said receiving section reads said private key, said public key information and said unique identifier from said cartridge, and effects said asymmetric encryption of said unique identifier using said private key.

4. An apparatus according to Claim 3,

wherein said cartridge includes a secure memory device;

wherein said private key, said public key information and said unique identifier are stored in said secure memory device; and

wherein said receiving section is operable to authenticate with said secure memory device in order to obtain access to the information stored therein.

5. An apparatus according to Claim 4,

wherein said unique identifier is also stored on said storage media during manufacture of said cartridge; and

wherein said receiving section compares said unique identifier stored on said storage media to said unique identifier stored in said secure memory device.

6. An apparatus according to Claim 3, wherein a private key list is maintained in a secure manner at a facility associated with cartridge manufacture, said private key list including a plurality of private keys and corresponding public key identifiers, said private key used for asymmetric encryption being one of said private keys selected from said private key list, and said public key information being the public key identifier corresponding to said selected private key.

7. An apparatus according to Claim 6,

wherein said further section includes a public key list containing a plurality of public keys;

wherein said public key information identifies one of said public keys in said public key list; and

wherein said further section uses said one public key to effect said decryption of said encrypted segment.

8. An apparatus according to Claim 3, wherein said further section is operable to transmit to said receiving section a request for said unique identifier, receipt of said request being said predetermined event.

9. An apparatus according to Claim 8,

wherein said further section places in said request a security code; and

wherein said receiving section includes said security code in said data segment in said encrypted segment transmitted to said further section in response to said request, said further section effecting a comparison of said security code sent in said request to said security code received in said data segment.

10. An apparatus according to Claim 9, including an additional section through which said further section and said receiving section communicate with each other, said additional section adding to said request a further security code, said receiving section including said further security code in said data segment in said encrypted segment, said additional section decrypting said encrypted segment as a function of said public key information, and said additional section effecting a comparison of said further security code sent in said request to said further security code received in said data segment.

11. An apparatus according to Claim 10,

wherein said further section and said additional section each include a public key list containing a plurality of public keys;

wherein said public key information identifies one of said public keys in said list; and

wherein said further section and said additional section each use said one public key to effect said decryption of said encrypted segment.

12. An apparatus according to Claim 10, wherein said comparison effected by said additional section includes comparison of each of said security codes from said request to a respective one of said security codes in said data segment.

13. An apparatus according to Claim 10,

wherein said security code included in said request by said further section is a substantially random number selected dynamically by said further section; and

wherein said further security code added to said request by said additional section is a substantially random number selected dynamically by said additional section.

14. An apparatus according to Claim 1,

wherein said encrypted segment and said public key information are stored in said cartridge during manufacture thereof; and

wherein said cartridge is free of said private key.

15. An apparatus according to Claim 14,

wherein said cartridge includes a secure memory device;

wherein said public key information and said encrypted segment are stored in said secure memory device; and

wherein said receiving section is operable to authenticate with said secure memory device in order to obtain access to the information stored therein.

16. An apparatus according to Claim 14, wherein a private key list is maintained in a secure manner at a facility associated with cartridge manufacture, said private key list including a plurality of private keys and corresponding public key identifiers, said private key used for asymmetric encryption being a selected one of said private keys from said private key list and said public key information being the public key identifier corresponding to said selected private key.

17. An apparatus according to Claim 16,

wherein said further section includes a public key list containing a plurality of public keys;

wherein said public key information identifies one of said public keys in said list; and

wherein said further section uses said one public key to effect said decryption of said encrypted segment.

18. An apparatus according to Claim 14,

wherein said unique identifier, a further private key, and further public key information are stored in said cartridge during manufacture thereof;

wherein said receiving section reads said further private key, said further public key information and said unique identifier from said cartridge;

wherein said receiving section forms a further data segment which includes said encrypted segment, said public key information associated with said encrypted segment, and said unique identifier;

wherein in response to said predetermined event said receiving section effects asymmetric encryption of said further data segment using said further private key to obtain a further encrypted segment;

wherein said receiving section transmits said further encrypted segment and said further public key information to said further section; and

wherein said further section decrypts said further encrypted segment as a function of said further public key information.

19. An apparatus according to Claim 18, wherein said receiving section compares said unique identifier from said further data segment with said unique identifier obtained by decrypting said encrypted segment in said further data segment.

20. An apparatus according to Claim 18,

wherein said cartridge includes a secure memory device;

wherein said encrypted segment, said public key information associated with said encrypted segment, said unique identifier, said further private key, and said further public key information are stored in said secure memory device; and

wherein said receiving section is operable to authenticate with said secure memory device in order to obtain access to the information stored therein.

21. An apparatus according to Claim 18,

wherein first and second private key lists are maintained in a secure manner at a facility associated with cartridge manufacture;

wherein said first private key list includes a plurality of first private keys and corresponding first public key identifiers;

wherein a selected one of said first private keys from said first private key list is said private key used for asymmetric encryption of said encrypted segment stored in said cartridge, and said corresponding public key information is the first public key identifier corresponding to said selected first private key; and

wherein said second private key list includes a plurality of second private keys and corresponding second public key identifiers, said private key used for asymmetric encryption of said further encrypted segment being a selected one of said second private keys from said second private key list and said further public key information being the second public key identifier corresponding to said selected second private key.

22. An apparatus according to Claim 21,

wherein said further section includes first and second public key lists which respectively contain a plurality of first and second public keys;

wherein said public key information associated with said encrypted segment stored in said cartridge identifies one of said public keys in said first public key list;

wherein said further public key information identifies one of said public keys in said second public key list; and

wherein said further section uses said one of said second public keys to decrypt said further encrypted segment and thereafter uses said one of said first public keys to decrypt said encrypted segment from said further data segment.

23. An apparatus according to Claim 18, wherein said further section is operable to transmit to said receiving section a request for said unique identifier, receipt of said request being said predetermined event.

24. An apparatus according to Claim 23,

wherein said further section places in said request a security code; and

wherein said receiving section includes said security code in said further data segment in said further encrypted segment transmitted to said further section in response to said request, said further section effecting a comparison of said security code sent in said request to said security code received in said further data segment.

25. An apparatus according to Claim 24, including an additional section through which said further section and said receiving section communicate with each other, said additional section adding to said request a further security code, said receiving section including said further security code in said further data segment in said further encrypted segment, said additional section decrypting said further encrypted segment as a function of said further public key information, and said additional section effecting a comparison of said further security code sent in said request to said further security code received in said further data segment.

26. An apparatus according to Claim 25,

wherein said further section includes first and second public key lists which respectively contain a plurality of first and second public keys;

wherein said additional section includes said second public key list;

wherein said public key information associated with said encrypted segment stored in said cartridge identifies one of said public keys in said first public key list;

wherein said further public key information identifies one of said public keys in said second public key list;

wherein said further section and said additional section each use said one of said second public keys to decrypt said further encrypted segment; and

wherein said further section uses said one of said first public keys to decrypt said encrypted segment from said further data segment.

27. An apparatus according to Claim 25, wherein said comparison effected by said additional section includes comparison of each of said security codes from said request to a respective one of said security codes in said further data segment.

28. An apparatus according to Claim 25,

wherein said security code included in said request by said further section is a substantially random number selected dynamically by said further section; and

wherein said further security code added to said request by said additional section is a substantially random number selected dynamically by said additional section.

29. A method, comprising the steps of:

associating a unique identifier with a cartridge having an information storage media therein;

providing a receiving section into which said cartridge can be removably inserted, said receiving section being operatively coupled to a further section;

responding to the occurrence of a predetermined event when said cartridge is removably inserted in said receiving section by causing said receiving section to transmit to said further section public key information and an encrypted segment, where said encrypted segment has been formed through asymmetric encryption with a private key of a data segment which includes said unique identifier; and

decrypting said encrypted segment in said further section as a function of said public key information, in order to obtain access to said unique identifier.

30. A method according to Claim 29,

including the step of maintaining in said further section a public key list containing a plurality of public keys, said public key information identifying one of said public keys in said list; and

wherein said decrypting step includes the step of using said one public key to effect said decryption of said encrypted segment.

31. A method according to Claim 29, including the step of:

storing said private key, said public key information and said unique identifier in said cartridge during manufacture thereof; and

causing said receiving section to read said private key, said public key information and said unique identifier from said cartridge, and effect said asymmetric encryption of said unique identifier using said private key.

32. A method according to Claim 31,

including the step of providing in said cartridge a secure memory device;

wherein said storing step is carried our by storing said private key, said public key information and said unique identifier in said secure memory device; and

including the step of causing said receiving section to authenticate with said secure memory device in order to obtain access to the information stored therein.

33. A method according to Claim 32, including the steps of:

storing said unique identifier on said storage media during manufacture of said cartridge; and

causing said receiving section to compare said unique identifier stored on said storage media to said unique identifier stored in said secure memory device.

34. A method according to Claim 31, including the step of maintaining a private key list in a secure manner at a facility associated with cartridge manufacture, said private key list including a plurality of private keys and corresponding public key identifiers, said private key used for asymmetric encryption being one of said private keys selected from said private key list, and said public key information being the public key identifier corresponding to said selected private key.

35. A method according to Claim 34, including the steps of:

maintaining in said further section a public key list containing a plurality of public keys, said public key information identifying one of said public keys in said public key list; and

causing said further section to use said one public key to effect said decryption of said encrypted segment.

36. A method according to Claim 31, including the step of causing said further section to transmit to said receiving section a request for said unique identifier, receipt of said request being said predetermined event.

37. A method according to Claim 36, including the steps of:

causing said further section to place in said request a security code;

causing said receiving section to include said security code in said data segment in said encrypted segment transmitted to said further section in response to said request; and

causing said further section to effect a comparison of said security code sent in said request to said security code received in said data segment.

38. A method according to Claim 37 including the steps of:

causing said further section and said receiving section to communicate with each other through an additional section;

causing said additional section to add to said request a further security code;

causing said receiving section to include said further security code in said data segment in said encrypted segment;

causing said additional section to decrypt said encrypted segment as a function of said public key information; and

causing said additional section to effect a comparison of said further security code sent in said request to said further security code received in said data segment.

39. A method according to Claim 38, including the steps of:

maintaining in each of said further section and said additional section a public key list containing a plurality of public keys, said public key information identifying one of said public keys in said public key list; and

causing each of said further section and said additional section to use said one public key to effect said decryption of said encrypted segment.

40. A method according to Claim 38, wherein said comparison step effected by said additional section includes the step of comparing each of said security codes from said request to a respective one of said security codes in said data segment.

41. A method according to Claim 38, including the steps of:

causing said further section to dynamically select a substantially random number for use as said security code included in said request by said further section; and

causing said additional section to dynamically select a substantially random number for use as said further security code added to said request by said additional section.

42. A method according to Claim 29, including the step of storing said encrypted segment and said public key information in said cartridge during manufacture thereof, said cartridge being free of said private key.

43. A method according to Claim 42, including the steps of:

providing a secure memory device in said cartridge;

carrying out said storing step by storing said public key information and said encrypted segment in said secure memory device; and

causing said receiving section to authenticate with said secure memory device in order to obtain access to the information stored therein.

44. A method according to Claim 42, including the step of maintaining a private key list in a secure manner at a facility associated with cartridge manufacture, said private key list including a plurality of private keys and corresponding public key identifiers, said private key used for asymmetric encryption being a selected one of said private keys from said private key list and said public key information being the public key identifier corresponding to said selected private key.

45. A method according to Claim 44, including the steps of:

maintaining in said further section a public key list containing a plurality of public keys, said public key information identifying one of said public keys in said list; and

causing said further section to use said one public key to effect said decryption of said encrypted segment.

46. A method according to Claim 42, including the steps of:

storing said unique identifier, a further private key, and further public key information in said cartridge during manufacture thereof;

causing said receiving section to read said further private key, said further public key information and said unique identifier from said cartridge;

causing said receiving section to form a further data segment which includes said encrypted segment, said public key information associated with said encrypted segment, and said unique identifier;

causing said receiving section to respond to said predetermined event by effecting asymmetric encryption of said further data segment using said further private key to obtain a further encrypted segment;

causing said receiving section to transmit said further encrypted segment and said further public key information to said further section; and

decrypting said further encrypted segment in said further section as a function of said further public key information.

47. A method according to Claim 46, including the step of comparing in said receiving section said unique identifier from said further data segment with said unique identifier obtained by decrypting said encrypted segment in said further data segment.

48. A method according to Claim 46, including the steps of:

providing in said cartridge includes a secure memory device;

carrying out said storing steps by storing said encrypted segment, said public key information associated with said encrypted segment, said unique identifier, said further private key, and said further public key information in said secure memory device; and

causing said receiving section to authenticate with said secure memory device in order to obtain access to the information stored therein.

49. A method according to Claim 46, including the steps of:

maintaining first and second private key lists in a secure manner at a facility associated with cartridge manufacture, said first private key list including a plurality of first private keys and corresponding first public key identifiers, and said second private key list including a plurality of second private keys and corresponding second public key identifiers;

selecting one of said first private keys from said first private key list to be said private key used for asymmetric encryption of said encrypted segment stored in said cartridge, said corresponding public key information being the first public key identifier which corresponds to said selected first private key; and

selecting one of said second private keys from said second private key list to be said private key used for asymmetric encryption of said further encrypted segment, said further public key information being the second public key identifier which corresponds to said selected second private key.

50. A method according to Claim 49, including the steps of:

maintaining in said further section first and second public key lists which respectively contain a plurality of first and second public keys, said public key information associated with said encrypted segment stored in said cartridge identifying one of said public keys in said first public key list, and said further public key information identifying one of said public keys in said second public key list; and

causing said further section to use said one of said second public keys to decrypt said further encrypted segment and to thereafter use said one of said first public keys to decrypt said encrypted segment from said further data segment.

51. A method according to Claim 46, including the step of transmitting from said further section to said receiving section a request for said unique identifier, receipt of said request being said predetermined event.

52. A method according to Claim 51, including the steps of:

causing said further section to place in said request a security code;

causing said receiving section to include said security code in said further data segment in said further encrypted segment transmitted to said further section in response to said request; and

causing said further section to effect a comparison of said security code sent in said request to said security code received in said further data segment.

53. A method according to Claim 52, including the steps of:

causing said further section and said receiving section to communicate with each other through an additional section;

causing said additional section to add to said request a further security code;

causing said receiving section to include said further security code in said further data segment in said further encrypted segment;

causing said additional section to decrypt said further encrypted segment as a function of said further public key information; and

causing said additional section to effect a comparison of said further security code sent in said request to said further security code received in said further data segment.

54. A method according to Claim 53, including the steps of:

maintaining in said further section first and second public key lists which respectively contain a plurality of first and second public keys, said public key information associated with said encrypted segment stored in said cartridge identifying one of said public keys in said first public key list, and said further public key information identifying one of said public keys in said second public key list;

maintaining in said additional section a duplicate of said second public key list;

causing said further section and said additional section to each use said one of said second public keys to decrypt said further encrypted segment; and

causing said further section to use said one of said first public keys to decrypt said encrypted segment from said further data segment.

55. A method according to Claim 53, including the step of carrying out said comparison effected by said additional section so as to include the step of comparing each of said security codes from said request to a respective one of said security codes in said further data segment.

56. A method according to Claim 53, including the steps of:

causing said further section to dynamically select a substantially random number for use as said security code included in said request by said further section; and

causing said additional section to dynamically select a substantially random number for use as said further security code added to said request by said additional section.